RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

UNIVERSITY POLICY

Section: 70.1.11

Section Title: Information Technology

Policy Name: Electronic Signatures

Formerly Book: N/A

Approval Authority: Executive Vice President and Chief Financial Officer

Responsible Executive: Senior Vice President and Chief Information Officer

Responsible Office: Office of Information Technology

Adopted:

Reviewed: NEW

Revised:

Contact: oit-policies@oit.rutgers.edu

1. **Policy Statement**

   This policy sets forth the requirements for the use of Electronic Signatures for all Rutgers, The State University of New Jersey documents that require a signature.

2. **Reason for Policy**

   To outline the requirements and process for the use of Electronic Signatures for University documents in accordance with the Uniform Electronic Transactions Act (UETA), N.J.S.A. 12:A-12-1 et seq. and ensure the trustworthiness of electronically signed University documents. The UETA encourages control processes and procedures appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and Auditability of Electronic Records. Use of Electronic Signatures generally increases the efficiency and timeliness in the signature process by reducing the need for printing and scanning documents. Electronic Signatures further promote University "green" initiatives by eliminating the need to create, mail, and store paper copies of documents.

3. **Who Should Read This Policy**

   All members of the University community including faculty, staff, students, covered entities, contractors, non-employees, and agents of the University.

4. **Resources**

   Policy 20.1.18: Construction Document Signatory

Policy 30.4.5 Records Management

Policy 50.3.13: Signatory Authority Policy (Signatory Delegation Policy)
Policy 70.1.1 Acceptable Use Policy for Information Technology Resources policy.

Uniform Electronic Transactions Act (UETA), N.J.S.A. 12:A-12-1 et seq.

5. **Definitions**

Audit or Auditability - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies, and operational procedures. [National Institute of Standards and Technology Special Publication 800-12 Rev. 1]

Authorization or Authorized - The process of verifying that a requested action or service is approved for a specific entity. Authorization to sign a University Document is derived from Policy 50.3.13: Signatory Authority Policy (Signatory Delegation Policy).

Electronic Signature - A paperless method used to approve or Authorize a document by indicating the person, or the entity on whose behalf the signer is Authorized to act, agrees to the content and meaning of the document, and that the University should be obligated to discharge any obligations specified in the document. An Electronic Signature that complies with the UETA has the same legal force and effect as a traditional "wet" signature. The UETA defines Electronic Signature as an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

Email (e-mail) - Messages distributed by electronic means from one computer user to one or more recipients via a network.

Procedures - Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

University Document - any contract or Agreement, memorandum of understanding, memorandum of agreement, grant instrument, application, letter, report, submission, or any other type of document that requires a signature by a natural person, regardless of the specific title of the document.

User - An individual granted access to systems or information to perform assigned duties.

Wet Signature – This term refers to signatures created on paper with the use of ink or a pen that dispenses wet ink (hence 'wet' signature). This is also referred to as a 'hand-written signature'.

6. **The Policy**

An Electronic Signature may be used/accepted in all situations when the requirement of a signature or approval is stated or implied, except when law, regulation, contract terms, or other stipulations specifically require a hand-written signature. To the fullest extent permitted by law, the University recognizes an Authorized Electronic Signature as legally binding. All members of the University community who are otherwise Authorized to sign a University document on behalf of the University are

encouraged to use Electronic Signatures created by an approved Electronic Signature software application when executing such University documents. An Electronic Signature will not be considered valid if the individual did not have the authorization to sign the University document in question and if a non-approved Electronic Signature software application was used (see 70.1.1-Acceptable Use Policy section 6.A.vii.). Notwithstanding the foregoing, where an Electronic Signature is not permitted or accepted by the University's counterparty or other third-party, or is not feasible or practical, a traditional "wet" signature is permissible.

This policy covers all uses of software for an electronic signature. This authorization extends beyond contract signing and encompasses various actions, ensuring compliance and endorsement for a range of activities aligned with the stipulations of the Policy 70.1.1 Acceptable Use Policy for Information Technology Resources policy.

Roles and Responsibilities

A. User responsibilities, include but are not limited to:
    a. Understand and comply with this policy and the University policies referenced herein;
    b. Understand and comply with all policies that govern acceptable use of organizational systems; and
    c. Use the organization-provided IT resources for defined purposes only.

B. Executive/Senior/Vice Presidents, Chancellors, Deans, Directors, and Department Chairs:
    a. Are responsible for safeguarding their organization's electronic information and information systems.
    b. Must ensure that each member of their organization understands the need to protect the University's electronic information and information systems.
    c. Must communicate this policy to all members of their organization.
    d. Must establish, maintain, and disseminate documentation, such as technology standards, procedures, and/or guidelines, to ensure compliance as stated in this Policy.

C. The Chief Information Officer, in consultation with the Chief Financial Officer, will determine which Electronic Signature software application(s) may be used for University Documents and will list the approved software application(s) on the Rutgers Information Technology website.

D. Any such Electronic Signature software application shall comply with the UETA and other applicable legal requirements.

E. Once one or more Electronic Signature software applications have been identified and installed for use at the University, all University employees who are otherwise Authorized to sign University Documents on behalf of the University shall use the application(s) so installed.

F. The Chief Information Officer may approve use of another Electronic Signature software application where required by the University's counterparty or other third-party so long as that substitute software meets the requirements of the UETA.

G. Questions regarding whether a counterparty's or third-party's Electronic Signature application can be used by University employees should be directed to the Chief Information Officer or his or her designee.

7. **Non-Compliance and Sanctions**

Failure to comply with this policy may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable State and federal statutes.